The New Data Marketplace: Protecting Personal Data, Electronic Communications, and Individual Privacy in the Age of Mass Surveillance Through a Return to a Property-Based Approach to the Fourth Amendment

by MEGAN BLASS*

I. Mass Surveillance in the New Millennium: Edward Snowden Versus The National Security Agency

A. Watergate Fears Realized: National Security Agency Programs Exposed in 2013

Edward Snowden is now a household name.[1] He garnered global attention in 2013 when he claimed responsibility for leaking government documents that revealed unprecedented levels of domestic surveillance conducted by the National Security Agency ("NSA" or "the Agency").[2] The information leaked by Mr. Snowden was just the tip of the iceberg. Since the initial leaks in June 2013, government documents have been unsealed, lawsuits have been filed, and alarming information about National Security Agency

* J.D. Candidate 2015, University of California, Hastings College of the Law. This Note is dedicated to Angelique Davis, Esq., Associate Professor, Department of Political Science, Seattle University for her inspirational scholarship and leadership, dedication to social justice, and unwavering support.

1. John Cassidy, *Snowden's Solution: More Encryption, Better Watchdogs*, NEW YORKER (March 10, 2014), *available at* http://www.newyorker.com/online/blogs/johncassidy/2014/03/snowdens-solution-more-encryption-and-better-watchdogs.html.

2. *See* Barton Gellman, Aaron Blake & Greg Miller, *Edward Snowden Comes Forward as Source of National Security Agency Leaks*, WASH. POST (June 9, 2013), *available at* http://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html.

surveillance has continued to come to light.[3] The 2013 leaks resulted in public outcry and calls for action from both sides of the political aisle.[4]

While discussion over the intelligence gathering programs administered by the National Security Agency exploded in 2013, concern over domestic spying is hardly a recent phenomenon.[5] As early as 1975, in the aftermath of the Watergate scandal, members of Congress were concerned about the National Security Agency's intelligence gathering programs.[6] Even then, members of Congress feared that the National Security Agency's intelligence gathering programs would be turned towards United States citizens and used in domestic spying operations.[7] Almost forty years later, such fears have come true. The 2013 leaks generated more questions than answers. What remains true is that the constitutional and regulatory framework governing personal data and electronic communications needs an overhaul. In an era of intrusive domestic surveillance, individuals should own property rights in their personal data and electronic communications in order to receive the protection they are truly entitled to under the Fourth Amendment.

3. *See Timeline of National Security Agency Domestic Spying*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/nsa-spying/timeline (last visited Jan. 30, 2015); *NSA Files: Decoded*, GUARDIAN, *available at* http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 (last visited Apr. 7, 2014); EDWARD C. LIU, ANDREW NOLAN & RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R43459, OVERVIEW OF CONSTITUTIONAL CHALLENGES TO NSA COLLECTION ACTIVITIES AND RECENT DEVELOPMENTS 8 (2014) (reviewing several instances of recent litigation over NSA surveillance).

4. Frank Newport, *Americans Disapprove of Government Surveillance Programs*, GALLUP (June 12, 2013), *available at* http://www.gallup.com/poll/163043/americans-disapprove-government-surveillance-programs.aspx.

5. *Timeline of National Security Agency Domestic Spying*, *supra* note 3.

6. *The National Security Agency and Fourth Amendment Rights: Hearings Before the Select Committee to Study Governmental Operations With Respect to Intelligence Activities*, 94th Cong. 1–3 (1975).

7. "We have a particular obligation to examine the NSA, in light of its tremendous potential for abuse. It has the capacity to monitor the private communications of American citizens without the use of a 'bug' or 'tap.' The interception of international communications signals sent through the air is the job of NSA; and, thanks to modern technological developments, it does its job very well. The danger lies in the ability of the NSA to turn its awesome technology against domestic communications." *Id.* at 2.

B. The National Security Agency is Collecting an Unprecedented Variety and Quantity of Personal Data, Virtual Information, and Electronic Communications

The National Security Agency conducts so much domestic surveillance that it would be easier to answer the question "what isn't the National Security Agency collecting" than to detail every facet of the Agency's intelligence gathering programs.[8] Recently, its PRISM and XKeyscore programs garnered notoriety. Through these programs, the National Security Agency has collected massive amounts of personal data and information, including the contents of e-mails, stored data, and internet traffic.[9] Even without PRISM and XKeyscore, the National Security Agency collects more than 250 million internet communications each year.[10] Moreover, even the Supreme Court has acknowledged the tremendous capability of the government to conduct this surveillance.[11]

1. PRISM

PRISM was one of the NSA programs revealed by Edward Snowden.[12] The PRISM program is a form of indirect surveillance that involves the NSA working with various internet-based service providers, including Google, Apple, and Facebook, to collect user information and communication content.[13] Through PRISM, the

8. The answer to that question, by the way, is not much.

9. *See National Security Agency slides explain the PRISM data-collection program*, WASH. POST (July 10, 2013), *available at* http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/; Ryan Gallagher, *National Security Agency Even Spied on Google Maps Searches, Documents Suggest*, SLATE (July 11, 2013), *available at* http://www.slate.com/blogs/future_tense/2013/07/11/xkeyscore_program_may_have_allowed_National Security Agency_to_spy_on_google_maps_searches.html; Barton Gellman & Todd Lindeman, *Inner workings of a top-secret spy program*, WASH. POST (June 29, 2013), *available at* http://apps.washingtonpost.com/g/page/national/inner-workings-of-a-top-secret-spy-program/282/; Barton Gellman & Ashkan Soltani, *National Security Agency Tracking Cellphone Locations Worldwide, Snowden Documents Show*, WASH. POST (Dec. 4, 2013), *available at* http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html; Ashkan Soltani & Matt DeLong, *FASCIA The National Security Agency's huge trove of location records*, WASH. POST (Dec. 4, 2013), *available at* http://apps.washingtonpost.com/g/page/world/what-is-fascia/637/# document/p1/a135288.

10. Memorandum Opinion and Order at 29, *In re* Government's *Ex parte* Submission of Reauthorization Certification and Related Procedures, Docket Number Redacted (FISA Ct. Oct. 3, 2011).

11. Clapper v. Amnesty Int'l, 133 S. Ct. 1138, 1158–59 (2013).

12. Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps into User Data of Apple, Google, and Others*, GUARDIAN 1 (June 6, 2013), *available at* http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

13. *Id.*

government has directly accessed email, chat, photos, stored data, voice over IP, and other information stored on participating companies' servers.[14] Although not explicitly a part of the PRISM program, the NSA has also engaged in bulk phone record collection.[15] Most notably, in 2013, Verizon was asked to turn over phone numbers, call durations, location data, and other customer information for all of its customers on a daily basis, including information about purely domestic calls.[16] These indirect surveillance programs were conducted pursuant to the Foreign Intelligence Surveillance Act § 702, but their domestic focus and use in ordinary domestic criminal prosecutions has caused alarm among civil libertarians and the public.[17]

2. Upstream Collection

The NSA has also been operating a program similar to PRISM involving upstream collection of communications on AT&T's network.[18] In one particular instance, the NSA installed a special room at AT&T's Folsom Street Facility in San Francisco, where all communications passing through the facility were "split," or redirected through the special room, so that they could be collected before reaching their destination.[19] Upstream collection was not limited to international communications or communications where one party to the communication was located abroad.[20] With this one facility, the NSA had access to 10% of all domestic internet communications in the United States.[21]

14. *Id.*

15. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN 1 (June 5, 2013), *available at* http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; Secondary Order at 1–3, *In re* Application of the Fed. Bureau of Investigation for the Production of Tangible Things from Verizon Business Network Services Inc. (FISA Ct. Apr. 25, 2013) (No. BR 13-80).

16. Secondary Order at 2, *In re* Application of the Fed. Bureau of Investigation for the Production of Tangible Things from Verizon Business Network Services Inc. (FISA Ct. Apr. 25, 2013) (No. BR 13-80).

17. *Id. See* Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1881 (2008).

18. Plaintiffs' Federal Rule of Evidence Section 1006 Summary of Voluminous Evidence Filed in Support of Their Motion for Partial Summary Judgment and Opposition to the Government Defendants' Cross-Motion at 4, Jewel v. Nat'l Sec. Agency, 965 F. Supp. 2d 1090 (N.D. Cal. 2013) (No. 08-04373).

19. *Id*. at 7.

20. *Id.*

21. *Id.* at 8–9.

3. XKeyscore

XKeyscore was one of the most far-reaching programs revealed by the Snowden leaks. The XKeyscore program compiled the many forms of content and metadata being mined by the NSA, such that a full data and content dossier on any individual could be accessed with the click of a button.[22] "The purpose of XKeyscore is to allow analysts to search the metadata as well as the content of emails and other internet activity, such as browser history, even when there is no known email account (a 'selector' in NSA parlance) associated with the individual being targeted."[23] XKeyscore includes social media activity and browsing data, which generally fall under the umbrella of personal data, similar to that which is traded by data mining and advertising agencies.

There is no doubt that the highly invasive programs conducted by the National Security Agency are an invasion of privacy. While conducting mass surveillance in the name of fighting international terrorism—but for the purposes of domestic or ordinary criminal prosecutions—is dishonest and disingenuous, it also poses a threat to our criminal justice system. The risk and actual use of evidence gathered pursuant to Foreign Intelligence Surveillance Act ("FISA") or Electronic Communications Privacy Act ("ECPA") but in violation of the Fourth Amendment, is serious.[24]

II. A Failed Framework: FISA, ECPA, and the Fourth Amendment Do Not Protect or Provide a Remedy

A. Domestic and International Surveillance Regulations Do Not Protect the Public Because They Require Less Stringent Standards than the Fourth Amendment

The National Security Agency's surveillance programs are typically subject to either ECPA or FISA.[25] Generally speaking, ECPA applies to domestic electronic surveillance or investigation,

22. Glenn Greenwald, *XKeyscore: NSA Tool Collects Nearly Everything a User Does on the Internet*, GUARDIAN (July 31, 2013), *available at* http://www.theguardian.com/world/ 2013/jul/31/nsa-top-secret-program-online-data.

23. *Id.*

24. *See* Kathlyn Querubin, *Cutting the Fourth Amendment Loose From Its Moorings: The Unconstitutional Use of FISA Evidence in Ordinary Criminal Prosecutions*, 37 HASTINGS CONST. L.Q. 371, 394–97 (2010).

25. *See* Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–22 (2011); Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1811. *See also* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1305 (2004).

while FISA applies when the government is gathering intelligence on foreign targets.[26] These statutes purport to place limitations on government surveillance. However, these statutes actually operate to reduce the burden the government must satisfy in order to engage in the type of investigation for the purposes of criminal prosecution generally governed by the Fourth Amendment.[27] Both statutes allow the government to conduct, what I argue should constitute, searches under the Fourth Amendment, in the absence of Fourth Amendment requirements including probable cause or the lower standard of reasonable suspicion and in the absence of a warrant.[28] Law enforcement should not be allowed to avoid the Fourth Amendment through the use of FISA.[29] While, in theory, these statutes regulate government surveillance of electronic communications and personal data, they provide little protection without compliance from agencies, such as the National Security Agency.

B. The Relevant Statues Fail to Protect the Public When Agencies Exceed Their Authority Under the Statutes

In *Jewel v. National Security Agency*, a lawsuit filed by the Electronic Frontier Foundation ("EFF"), a putative class of plaintiffs made up of AT&T customers sought legal and equitable relief for violations of federal constitutional rights, FISA, and ECPA.[30] They alleged that the NSA, in cooperation with AT&T, engaged in the collection of communications passing through AT&T's network at its Folsom Street Facility without satisfying the FISA and ECPA requirements of reasonable suspicion that the target is a foreign power or agent and reasonable suspicion that the information is relevant to a criminal investigation or to an investigation to protect against international terrorism and spying.[31] Many of the EFF's

26. Solove, *supra* note 25, at 1266.

27. *See* Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, 4 (2007); Patricia L. Bellia & Susan Freiwald, *Law in a Networked World: Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121, 122 (2008); Querubin, *supra* note 24, at 372–74; Michael P. O'Connor & Celia Rumann, *Going, Going, Gone: Sealing the Fate of the Fourth Amendment*, 26 FORDHAM INT'L L.J. 1234 (2003); William Pollak, *Shu'ubiyya or Security? Preserving Civil Liberties by Limiting FISA Evidence to National Security Prosecutions*, 42 U. MICH. J. L. REFORM 221, 221–23 (2008).

28. Freiwald, *supra* note 27, at 4; Querubin, *supra* note 24, at 373.

29. Pollak, *supra* note 27, at 222–23.

30. Complaint for Constitutional and Statutory Violations, Seeking Damages, Declaratory, and Injunctive Relief at 25–34, Jewel v. Nat'l Sec. Agency, 965 F. Supp. 2d 1090 (N.D. Cal. 2013) (No. 08-04373).

31. *Id.* at 13–14. *See* 50 U.S.C. §§ 1802(a)(1)(A)–(C).

allegations are supported by credible evidence and have been admitted, to some extent, by the government.[32] This lawsuit and other lawsuits filed over the last five years demonstrate that, regardless of the constitutionality of FISA or ECPA, FISA and ECPA provide little protection for the public when the government refuses to adhere to them.[33]

ECPA and FISA are supposed to limit the collection and use of personal data and electronic communications.[34] The National Security Agency's mass surveillance programs, conducted pursuant to ECPA and FISA, however, have swept up massive amounts of data and content that would be ancillary to any individual application for a wiretap. While this is a tremendous invasion of privacy, the crux of the constitutional issue is that limits on the use of that data and information have proven to be ineffective. So, not only is the NSA abrogating its front end responsibilities and obligations under ECPA and FISA in operation of its mass surveillance programs, the data and content are in turn being improperly utilized in ordinary criminal prosecutions without any fallback protection from the Fourth Amendment. Failure to comply with FISA and the ECPA is what makes the Court's Fourth Amendment jurisprudence so critical. The Fourth Amendment is the legal protection of last resort where Congress's statutory protections have failed. It is the ultimate backstop.[35]

C. The Supreme Court's Fourth Amendment Jurisprudence Does Not Adequately Protect the Rights and Interests of the Public Because it Excludes Modern Means of Communication and Data Generated Through the Use of Web-Based Applications

While the NSA continues to disregard statutes such as FISA and ECPA, the public is left with little protection by way of the Constitution as currently interpreted by the Supreme Court. The Constitution, which sets the floor for government behavior where

32. Plaintiffs' Federal Rule of Evidence Section 1006 Summary of Voluminous Evidence Filed in Support of Their Motion for Partial Summary Judgment and Opposition to the Government Defendants' Cross-Motion at 4, Jewel v. Nat'l Sec. Agency, 965 F. Supp. 2d 1090 (N.D. Cal. 2013) (No. 08-04373).

33. *See* LIU, NOLAN & THOMPSON II, *supra* note 3, at 8 (reviewing several instances of recent litigation over NSA surveillance).

34. *See* Querubin, *supra* note 24, at 372–74.

35. *See also* Freiwald, *supra* note 27, at 4 (stating that the lack of a statutory suppression remedy under the ECPA means that victims of illegal digital surveillance and electronic eavesdropping can only obtain relief if they prevail on a claim of Fourth Amendment violation).

Fourth Amendment rights are implicated, provides almost no protection from unreasonable searches and seizures or the use of evidence illegally obtained by the NSA in criminal prosecutions.[36] The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[37]

The text of the Fourth Amendment enumerates different property items, the enumeration of which has given rise to a long-standing property-based approach to the Fourth Amendment.[38] As early as 1886, the Court interpreted a search under the Fourth Amendment as occurring when the government violated a property interest, such as physical intrusion into the home or review of one's personal documents.[39] While the Court has explicitly refrained from overruling this trespass theory of the Fourth Amendment, it is no longer the only controlling doctrine.[40]

In *Katz v. United States*, the Court took steps to adopt a privacy-based approach to the Fourth Amendment instead of a formalistic property-based approach.[41] In *Katz*, the majority, led by Justice Stewart, held that the Fourth Amendment protects people, not just constitutionally protected areas, and accordingly, that a search takes place where the government violates an individual's privacy.[42] The *Katz* approach that the Court has adopted since rendering a decision

36. *See, e.g.*, Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 106–07 (2008); Freiwald, *supra* note 27.

37. U.S. CONST. amend. IV.

38. *Id.*; United States v. Jones, 132 S. Ct. 945, 949–50 (2012); Kyllo v. United States, 533 U.S. 27, 31 (2001); Silverman v. United States, 365 U.S. 505, 511 (1961).

39. Boyd v. United States, 116 U.S. 616, 622 (1886). *See also Jones*, 132 S. Ct. at 949 (quoting Entick v. Carrington, 95 Eng. Rep. 807 (C.P. 1765)) ("Our law holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without his leave; if he does he is a trespasser, though he does no damage at all; if he will tread upon his neighbour's ground, he must justify it by law.").

40. *Jones*, 132 S. Ct. at 950–52 (holding that *Katz v. United States* was an addition to, and not replacement of, Fourth Amendment protection of property).

41. Katz v. United States, 389 U.S. 347, 350–52 (1967).

42. *Id.* at 353.

in the case is actually the approach articulated by Justice Harlan in his concurring opinion in *Katz*.[43] The often-cited rule as formulated by Harlan, and adopted by the Court, states that a search occurs when there is an intrusion upon an expectation of privacy that society is prepared to recognize as reasonable.[44] *Katz* seems to be a reasonable expansion of Fourth Amendment protection on its face; after all, it sought to protect people as well as property. In attempting to interpret a reasonable expectation of privacy, the Court has faltered.

In *Smith v. Maryland*, a pen register, which is a device that records the numbers dialed on a phone, was used to investigate Michael Lee Smith for the purposes of a criminal prosecution.[45] Under *Katz* and its progeny, a person does not have a legitimate expectation of privacy in information voluntarily disclosed to a third party.[46] The Court held that the use of the pen register was not a search within the meaning of the Fourth Amendment because Smith did not have a reasonable expectation of privacy in the numbers he dialed, as they were transmitted through a third party.[47] *Smith* has serious implications in the digital age.[48] The third party doctrine eviscerates Fourth Amendment protection under *Katz* in the modern age. Through one decision, the Court brought nearly all modern methods and modes of communication outside the operation of the Fourth Amendment.[49] Through its holding in *Smith v. Maryland*, the Court did not just refuse to extend Fourth Amendment protection in one particular instance or create an exception. *Smith* made it such that surveillance and investigation involving collection or review of communications or data that have passed through an internet service provider, a precondition satisfied anytime the internet is involved, do not constitute searches.[50] As Justice Sotomayor pointed out in her concurrence in *United States v. Jones*, the third party doctrine is "ill

43. *Id.* at 361 (Harlan, J., concurring); *Jones*, 132 S. Ct. at 950.

44. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

45. Smith v. Maryland, 442 U.S. 735, 737 (1979).

46. *Id.* at 743–44. *See also* United States v. Miller, 425 U.S. 435, 442–44 (1976) ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government . . . This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

47. *Smith*, 442 U.S. at 745–46.

48. *Jones*, 132 S. Ct. at 955–57 (Sotomayor, J., concurring).

49. *See* 1 HALL, SEARCH & SEIZURE § 5.03 (2013).

50. Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1, 1–2 (2013).

suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[51] Without a reasonable expectation of privacy in the data and communications collected by the NSA, the alternative source of Fourth Amendment protection is the Court's classic trespass theory. Absent congressional intervention in the form of legislation vesting property rights in electronic communications and personal information, the Court's trespass theory fails to provide any protection either.[52]

In *United States v. Jones*, law enforcement personnel, in the course of a criminal investigation, placed a GPS tracking device in the undercarriage of Antoine Jones's publicly parked car and tracked the movements of the vehicle for four weeks.[53] The Fourth Amendment provides that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[54] The term "effects," as used in the Fourth Amendment, is understood to include automobiles.[55] The Court concluded that the placement of the GPS tracker in the undercarriage of Mr. Jones's car constituted a search under the Fourth Amendment because an automobile, as an effect, is a constitutionally protected entity, and the placement of the GPS tracker was a physical intrusion into that constitutionally protected area.[56]

In *Kyllo v. United States*, the Court considered the constitutionality of thermal imaging technology.[57] In that case, police used a thermal imaging device not generally available to the public in order to discern the presence of heat within the interior of the house they were surveilling.[58] The device the police used was capable of detecting infrared radiation inside the house from all the way across the street, such that the investigating officers did not even need to leave their vehicle.[59] The Court held that the use of technology not generally available to the public, such as the thermal imaging used by

51. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring); Bedi, *supra* note 50, at 3.

52. *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) (articulating that modern surveillance technologies no longer require a physical intrusion).

53. *Id.* at 947–48.

54. U.S. CONST. amend. IV.

55. United States v. Chadwick, 433 U.S. 1, 12 (1977).

56. *Jones*, 132 S. Ct. at 949.

57. *Kyllo*, 533 U.S. at 29–30.

58. *Id.*

59. *Id.*

the investigating officers, in order to ascertain intimate details of a home not knowable without physical intrusion into the home constituted a search.[60]

In *Florida v. Jardines*, the Court once again considered a use of novel technology under its trespass theory of the Fourth Amendment.[61] In this case, police, on the basis of an uncorroborated tip, went to the home of Joelies Jardines in order to look for evidence of marijuana cultivation.[62] They utilized a dog specially trained to detect and alert to certain odors, including those of narcotics.[63] The police allowed the dog to walk near and around the door to Jardines's home, where the dog gave an alert, which subsequently served as the basis for a warrant to search the residence.[64] Applying its trespass theory, the Court, in an opinion by Justice Scalia, held that the use of the drug sniffing dog constituted a search under the Fourth Amendment because the dog intruded upon a constitutionally protected area, the curtilage, which is afforded the same protection as the home itself.[65]

Jones, *Kyllo*, and *Jardines* are significant because they represent instances of the Court applying its trespass theory in order to determine the constitutionality of modern surveillance techniques that are less physically intrusive. *Jones* is particularly significant because it was recent. The Court has consistently stated that its privacy approach under *Katz* was in addition to its trespass theory.[66] *Jones* demonstrates, that while the Court has used *Katz*, it is more comfortable applying the traditional trespass theory, even in 2012.[67] While *Jones* is a recent example of the Court protecting Fourth Amendment rights on the basis of its trespass theory, the Court has not had much occasion to apply the trespass theory to the types of electronic surveillance being conducted by the NSA. To be sure, while *Jones* did involve technology, ultimately, the trespass doctrine applied because it also involved the placement of a physical device on

60. *Id.* at 40.

61. Florida v. Jardines, 133 S. Ct. 1409, 1413 (2013).

62. *Id.*

63. *Id.*

64. *Id.*

65. *Id.* at 1416–18.

66. *Jones*, 132 S. Ct. at 950–52 (holding that *Katz* was an addition to, and not replacement of, Fourth Amendment protection of property).

67. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 809 (2004).

a vehicle, which provided the Court with a way to tether the GPS technology to its trespass theory.

The thermal imaging device considered by the Court in *Kyllo* is the closest surveillance technique to the mass collection and review of e-mails, text messages, browsing histories, and keystrokes the Court has considered on the merits.[68] The Court's jurisprudence has not, up to this point, provided any affirmative protection of electronic communications and personal data under its trespass theory. It is unclear whether or not the Court would extend its trespass jurisprudence to instances of police investigation that did not involve some sort of literal physical intrusion, as in *Jones*, or effective physical intrusion of the home specifically, as in *Kyllo*.[69] Vesting property rights in personal data and electronic communications will provide the Court with a tangible foundation for applying its trespass theory.

III. A Property-Based Framework under the Fourth Amendment

A. Vesting Property Rights in Personal Data and Electronic Communications Will Facilitate a Fair Marketplace and Fourth Amendment Protection

Since the proliferation of personal computing and the internet, scholars, economists, and public advocates have discussed the merits of granting individuals property rights in their personal data and virtual identification information.[70] Much of the discussion over vesting property rights in personal data has concerned promoting privacy and creating a fair and efficient marketplace for personal data.[71] From the perspective of many economists, there is currently a market failure occurring in the marketplace for personal data.[72] While firms that use and sell personal data take advantage of the full

68. *See Kyllo*, 533 U.S. at 29–30 (describing sense-enhancing technology used to assess infrared radiation at the residence of Petitioner, Danny Kyllo).

69. *See* Dow Chem. v. United States, 476 U.S. 227, 236–38 (1986) (holding that the space surrounding commercial buildings are neither analogous to nor entitled to the same protection as the curtilage of a home or dwelling).

70. *See* Kenneth C. Laudon, *Markets and Privacy: Privacy Regulation in National Networks*, 39 COMM. OF THE ASS'N FOR COMPUTING MACH. 92, 93 (1996); Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 74–78 (1996); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1132.

71. Samuelson, *supra* note 70, at 1128; Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381 (1996).

72. Samuelson, *supra* note 70, at 1127–28.

benefit of trading in such data, they bear none of the costs, costs that are externalized and borne out by consumers whose data is overexposed without their knowledge or consent.[73] Some argue that granting individuals property rights in their personal data will empower them to engage in the bargaining necessary to protect their privacy and to hold firms trading consumer data to a reasonable standard governing the dissemination, disclosure, and sale of such information and data.[74] In addition to these positive outcomes, granting individuals property rights in their personal data will also facilitate the protection of Fourth Amendment rights. As I will discuss, property rights will facilitate judicial application of the trespass theory of the Fourth Amendment. However, property rights, or a licensing scheme such as the one advocated for by Pamela Samuelson, could also open the door to reform of the third party doctrine.

Scholars advocating for a more equitable marketplace for personal data have articulated that fortifying individuals' rights to personal data will facilitate a system where individuals can choose to maintain the privacy of their information or disclose it as they see fit.[75] The bargaining that will take place in a licensing or property-based scheme will serve as evidence of whether or not an individual intended to maintain the confidentiality of his or her information, or more specifically, the precise terms of their disclosure to a third party. The presence of bargaining and the terms of disclosure could serve as a factual basis for the Court to conduct a more reasonable evaluation of the degree to which information has been exposed to the public. It would be untenable for the Court to continue to hold that third party disclosure is public information where consumers have the ability to not only opt for confidentiality, but to prescribe the terms of use and disclosure of their personal information. Rather than try to interpret expectations of privacy, the Court would have the capability to look to actual agreements between the parties. Property rights in personal data may have the side effect of facilitating a more coherent analysis under *Katz* and *Smith v. Maryland*; however, a return to a trespass theory of the Fourth Amendment is still preferable. While rehabilitating the third party doctrine would require a Court that was actually willing to revisit the doctrine and deviate from *stare decisis* in

73. PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 8 (1998). *See also* Samuelson, *supra* note 70, at 1128, 1132–33.

74. Laudon, *supra* note 70, at 93; Murphy, *supra* note 71, at 2406.

75. Laudon, *supra* note 70, at 93; Mell, *supra* note 70, at 79.

a substantial number of cases, there is a workable way for the Court to apply its existing trespass jurisprudence.

Vesting property rights will provide the Supreme Court with the necessary property interest to anchor its trespass theory of the Fourth Amendment. *Smith v. Maryland* removed personal data and electronic communications from the scope of the Fourth Amendment, but a concrete property right will bring that content and information back within the operation of the Fourth Amendment.[76] Giving individuals property rights in their personal data and electronic communications renders what was once intangible and outside the scope of the trespass theory tangible and concrete, such that a trespass theory can properly be applied both in law and in fact. The Court has demonstrated its willingness to maintain and apply its trespass theory of the Fourth Amendment in instances where there is a physical and tangible way to tie that theory to the facts of the case.[77] When individuals have ownership of their personal data and electronic communications, they will have the power to truly control the disclosure and use of that information and will provide the Court with a clear way to examine instances of police investigation and surveillance. Where there are property rights in personal data and electronic communications, the Court has the ability to look at the alienation of that information and content as a property right rather than trying to analyze the degree to which information has been exposed when disclosed to one party.

In contrast to the eviscerated Fourth Amendment protection under *Katz* as interpreted in *Smith v. Maryland*, the trespass theory of the Fourth Amendment as applied to personal data and electronic communications provides significantly more protection. This is principally because under a trespass theory, the Court looks at the steps taken to protect the property from prying eyes, rather than presuming public disclosure where there has been disclosure to even one third party.[78] As early as 1886, the Court recognized the common law definition of curtilage as an area closely tied to the "sanctity of a man's home and the privacies of life."[79] Later, the Court elaborated on this concept by holding that the curtilage is an extension of the home where intimate activities may transpire, such that the curtilage

76. *See Smith*, 442 U.S. at 745–46.

77. *See, e.g.*, *Jones*, 132 S. Ct. at 949.

78. United States v. Dunn, 480 U.S. 294, 301 (1987) (holding there are four factors to consider in order to determine the curtilage of a home); *Smith*, 442 U.S. at 745–46 (holding no expectation of privacy in information disclosed to third party).

79. *Boyd*, 116 U.S. at 630.

is considered to be part of the home itself under the Fourth Amendment.[80]

In contrast to the protected curtilage area are open fields, which are considered to be public.[81] In *Hester v. United States*, a prohibition era case, the police obtained evidence that the defendant had moonshine when a jug and bottle that had been discarded in hot pursuit were found outside of the defendant's home.[82] The Court held that the Fourth Amendment protections that applied to the enumerated categories of persons, houses, papers, and effects did not apply to open fields, or unenclosed areas away from the entrance to the home.[83] *Hester* allows police to enter and investigate an open field because doing so is not a search within the meaning of the Fourth Amendment.[84]

Personal data and electronic communications, such as the bulk collected by the NSA, are an extension of the individual and the home, and should be protected as such.[85] Like the activities that may take place in the curtilage of a home, personal data and electronic communications are closely tied to the privacies of life or intimate activities that are traditionally associated with the home.[86] An individual's search history, key strokes, personal data, and electronic communications and documents are all intimate activities, like those activities the Court is concerned with protecting under the Fourth Amendment. Intimate details of a person's life, all which may have had a concrete existence in a home during eras past now exist in virtual form. Financial information, communications between individuals and their closest friends and family, book, music, and movie collections are often stored on hard memory or in web-based applications such as TurboTax, Google, or iCloud. While the physical form of intimate activities and information associated with the home may have changed, these activities and information are conceptually the same and deserve continued protection under the Fourth Amendment.

80. Oliver v. United States, 466 U.S. 170, 180 (1984).

81. *Id.* at 171.

82. Hester v. United States, 265 U.S. 57, 57 (1924).

83. *Id.* at 59.

84. *Oliver*, 496 U.S. at 171.

85. "But when it comes to the Fourth Amendment, the home is first among equals. At the Amendment's 'very core' stands 'the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion." *Jardines*, 133 S. Ct. at 1414 (quoting *Silverman*, 365 U.S. at 511).

86. *See Kyllo*, 533 U.S. at 38 (describing personal routines, such as the time one takes a bath or sauna, as intimate details).

The Court has held that what separates the curtilage from public space or vantage points are an individual's attempts to protect the area and prevent trespass.[87] There are four factors the Court considers when determining whether or not to protect any area as part of the curtilage of the home.[88] The Court looks at the proximity between the area claimed as curtilage and the home, whether or not the claimed area is enclosed or fenced in, how the claimed area is used, and whether or not steps have been taken to protect the claimed area from observation by the public.[89] While in a real property context, these factors recognize the curtilage as an area immediately surrounding the home that is enclosed by fences or barriers, used for intimate activities, and protected by "no trespassing" signs or other measures to discourage public viewing, these same factors can be easily applied to personal data and electronic communications as well.

The first three factors of the Court's curtilage analysis go hand-in-hand. Posting publicly on a forum or blog generates content and data, but does so in the open and in a manner that is distant from one's metaphorical home on the internet. Additionally, posting in open forums means that the information and data generated by the posting are not walled off from the rest of the internet, and also, that the posting is not of a particularly intimate nature; otherwise it likely would not have been placed into the open web. In contrast, banking online or using online tax preparation or investment applications is closer in proximity to one's internet home. Financial information is quite intimate and would likely be maintained within the home itself. Additionally, the sort of web-based applications that are used to handle financial information are not like an open field, or its internet equivalent, an online forum. Instead, they are walled off, and data entered into such web-based applications is enclosed within the application, and typically encrypted, such that it is walled off from the rest of the internet.

Applying the fourth factor, it is very clear that individuals take steps to protect their information on the internet just as individuals might fence off real property and take steps to prevent the public or passersby from viewing the curtilage of their homes. The use of privacy settings, screen names, and passwords are all steps taken to protect the intimate details of an individual's internet activities and electronic communications. Additionally, private browsing, do-not-

87. *Dunn*, 480 U.S. at 301.

88. *Id.*

89. *Id.*

track settings, and alternatives to traditional internet browsing, such as Tor have developed to allow people to shield their intimate internet activities and browsing histories from the world.[90] Where an individual has not taken advantage of measures to protect his or her privacy and where that data or communication, perhaps in the form of a public Facebook post, has been placed into the open internet, the high degree of protection provided to the home and the curtilage should not be extended, as it is effectively information in an "open field."[91]

Applying the four factor curtilage test to the mass surveillance programs being operated by the NSA, the majority of the information being gathered, such as the content of electronic communications as well as information gained through bypassing password protection and directly accessing internet service provider and web-based application servers, would at the very least be subject to the Fourth Amendment where individuals have an actual property interest in that personal data and content. Where the NSA went around a firewall or password protection, or otherwise trespassed upon that electronic property, a physical intrusion will have taken place, which is a search under the Fourth Amendment.[92]

Where an individual has disclosed information to a third party, Fourth Amendment protection will not be completely eviscerated, at least under a trespass theory. While privacy policies represent an analog to agreements over the use of personal data and electronic communications as property, the Court has not treated them with the same degree of reverence.[93] Providing an internet service provider with information may nullify a privacy interest in that information, but disclosure of information would not nullify a property interest, rather, such a disclosure would be an exercise of the property owner's right to alienate the property.[94] Disclosure of information to which an individual has a property interest is akin to a bailment, which may be limited by certain terms and conditions, but unlike a privacy interest

90. Alex Fowler, *Congratulations, Chrome Users*, MOZILLA PRIVACY BLOG (Sep. 14, 2012), https://blog.mozilla.org/privacy/2012/09/14/congratulations-chrome-users/. *See also* Stuart Dredge, *What is Tor? A Beginner's Guide to the Privacy Tool*, GUARDIAN (Nov. 5, 2013), *available at* http://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser.

91. *See Hester*, 265 U.S. at 59.

92. *Jones*, 132 S. Ct. at 949.

93. *See* ACLU v. Clapper, 659 F. Supp. 2d 724, 749–51 (2013) (upholding the third party doctrine).

94. *See* 8A Am. Jur. 2d Bailments § 1 (2014).

under *Smith v. Maryland*, a property interest is not extinguished by an act of bailment or tenancy alone.[95]

There are several other ways that personal data and electronic communications would receive more protection under a property-based analysis under the Fourth Amendment. The Supreme Court has held that vehicles and other miscellaneous personal belongings constitute effects for purposes of the Fourth Amendment.[96] Establishing property rights in personal data would render data personal property properly considered an effect, which is constitutionally protected under the Fourth Amendment. Similarly, e-mail would properly be considered papers, which are an enumerated category of constitutionally protected property.[97] The creation of property rights in personal data and electronic information including social media activity, browsing history, and other metadata collected by the National Security Agency would not necessarily dispose of the constitutionality of those practices. The constitutionality of FISA, ECPA, and electronic surveillance conducted pursuant to those statutes is an entirely separate matter; however, it would at least subject such surveillance to the strictures of the Fourth Amendment. While e-mail and personal data would not be protected under a *Katz* theory due to the third party doctrine, they would be properly protected as papers and effects under the Court's longstanding trespass theory of the Fourth Amendment if a property right were to be created and vested.[98]

B. The Court Can Easily Apply Its Current Jurisprudence to Vested Property Rights in Personal Data and Electronic Communications

The ease with which the Court's existing trespass jurisprudence can be applied to personal data and electronic communications demonstrates that vesting property rights in those intangibles in order to facilitate application of the trespass theory will provide more Fourth Amendment protection. Analyzing surveillance of e-mail and other electronic communications under a trespass theory would be novel in the criminal context, but not in the civil context, which further demonstrates the ease by which the Court could apply its

95. *Id.*

96. *See Chadwick*, 433 U.S. at 12.

97. *See Ex parte* Jackson, 96 U.S. 727, 733 (1877); Walter v. United States, 447 U.S. 649, 654 (1980).

98. *See* Courtney M. Bowman, *A Way Forward After* Warshak*: Fourth Amendment Protections for E-mail*, 27 BERKELEY TECH. L.J. 809, 813–14 (2012) (identifying the third party doctrine's impact on Fourth Amendment protection of email).

trespass theory of the Fourth Amendment to electronic communications and personal effects.[99] A return to a property basis is valuable for additional reasons, however.

C. Property Law Concepts More Accurately Represent Public Conceptions of Electronic Communications, Personal Data, and Other Intangible Internet-Based Information

Property law is a good fit for electronic communications and personal data for several reasons. First of all, people conceive of their emails and personal data as property.[100] Like tangible personal effects, individuals generally have the right to exclude others from accessing their digital communications and personal data, even when it is in the custody of a third party, such as a hospital or financial institution.[101]

Harmony between the law and public expectations of what the law should be is important for the integrity of the Fourth Amendment, the courts, and our judicial system. As Lon Fuller articulated in his famous book, *The Morality of Law*, there is a reciprocal relationship between the government and the public, and where the public does not feel the laws are just or that the government will honor them, the citizen's fidelity to the law will be tested.[102] If people conceive of their personal data and electronic communications as property, then a congruent legal framework would vest individuals with property rights in that content, or as Patricia Mell describes it, their "electronic persona."[103]

Paradoxically, while individuals may conceive of their personal data and electronic communication as property, the ability to restrict access and the disclosure restrictions and procedures imposed upon third parties in possession of such personal information are largely rooted in concepts of privacy, not property.[104]

99. *See* Marjorie A. Shields, *Annotation, Applicability of Common-Law Trespass Actions to Electronic Communications*, 107 A.L.R 549 (2003).

100. Samuelson, *supra* note 70, at 1130.

101. *Id.*

102. LON L. FULLER, THE MORALITY OF LAW 39–41 (rev. ed. 1969)

103. *See* Mell, *supra* note 70.

104. Samuelson, *supra* note 70, at 1131.

D. Alternatively, Courts Can Seamlessly Extend the Existing Trespass Theory of the Fourth Amendment Without Additional Congressional Intervention or Upheaval of Established Precedent

Alternatively, absent congressional intervention through the creation of property rights, the Court could extend its trespass theory of the Fourth Amendment as established in *Kyllo*.[105] *Kyllo* is an example of the Court extending its trespass doctrine to a case where there was not necessarily a literal physical intrusion, but rather, where the use of technology effected a physical intrusion.[106] It would not be much more of a stretch for the Court to apply its holding to the NSA programs that came to light in 2012. PRISM, XKeyscore, and upstream collection programs utilize technology, as well as knowledge, that is not generally available to the public. Certainly some highly skilled individuals may have the ability to obtain the same information as the NSA through hacking or other unauthorized means of accessing information held by internet service providers and telecommunications companies. The ability of a few is not the same as widespread availability of a specific skill or technology. Additionally, the fact that these programs and surveillance methods have been classified and kept secret for so long further demonstrates that these technologies are not widely available to the general public, and are more analogous to the sense-enhancing technology used in *Kyllo* than mere public observation by law *enforcement.*[107]

As in *Kyllo*, the NSA's surveillance programs collect information not generally available to the public.[108] Additionally, the information that is collected likely could not be collected without virtual intrusion, or trespass, upon property rights vested in personal data and electronic communications.[109] With PRISM, the NSA had to request access to the servers of large tech companies in order to gain access to the data and content they sought.[110] The general public does not have access to these servers and does not have the ability to compile the quantity and quality of data that is being compiled through the XKeyscore program.[111] In this way, modern surveillance is just like *Kyllo*. The government is using sophisticated technologies to access

105. *See Kyllo*, 533 U.S. at 40.

106. *Id.*

107. *See supra* note 2.

108. *See supra* notes 12, 15–16, 22 (detailing electronic communications content and metadata collected by NSA).

109. *Id.*

110. *Supra* notes 12–17 (explaining the mechanics of the PRISM program).

111. Greenwald, *XKeyscore*, *supra* note 22.

intimate information about the public that they would not otherwise have access to if it were not for their use of the sophisticated, or sense-enhancing, technologies.

IV. A Trespass Approach to the Fourth Amendment is Preferable to *Katz* and Any Attempts to Reform a Privacy-Based Theory of the Fourth Amendment

Criticism of the third party doctrine among scholars and legal practitioners is nothing new.[112] Since the original revelation of the government's warrantless wiretapping programs there has been a flurry of scholarship declaring the end of privacy and examining reasonable expectations of privacy under *Katz*.[113] Privacy theory and jurisprudence is *en vogue* right now, but it will never provide as satisfactory of a solution to what ails the Fourth Amendment as a trespass theory.[114] This is because the *Katz* doctrine was not a workable standard to begin with.[115] The only way that *Katz*, a judicially created standard, can be rehabilitated, is if the Court, of its own volition, chooses to explicitly or implicitly overturn precedent such as *Smith v. Maryland*.[116] To square the reasonable expectations of privacy in various scenarios with the public's actual expectations of privacy in the digital age would require the Court to hear and decide many cases, some of which have not even begun to wind their way through the courts, and could never wind their way through the courts at the same rate of ever-evolving technology. Ultimately, *Katz* should not be rehabilitated because it was not a workable doctrine to begin with.

First, the Court is in a poor position to determine what privacy expectations society is prepared to recognize as legitimate.[117] Progress

112. James J. Tomkovicz, *Beyond Secrecy for Secrecy's Sake: Toward an Expanded Vision of the Fourth Amendment Privacy Province*, 36 HASTINGS L.J. 645, 681 (1985).

113. *See, e.g.*, Rubenfeld, *supra* note 36, at 106–07.

114. William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1047–51 (1995).

115. "The problem with the reasonable expectation of privacy test in the communications context is not that it requires judicial discretion, but that it requires both a positive and normative inquiry that challenges courts' competence. Moreover, the test, as courts currently interpret it, misplaces the focus onto what the target knew or should've known instead of on the intrusive nature of the surveillance itself." Freiwald, *supra* note 27, at 21.

116. *See, e.g.*, *ACLU v. Clapper*, 959 F. Supp. 2d at 752.

117. *See* Michele Estrin Gilman, *The Class Differential in Privacy Law*, 77 BROOK. L. REV. 1389, 1411–12 (2012) (arguing reasonable expectations of privacy preference the wealthy and landowners).

has been made in diversifying the bench, but Supreme Court justices still come from a particularly privileged segment of society and apply precedent crafted over hundreds of years by an even less diverse bench.[118] Of the current justices, all nine attended Ivy League law schools, primarily Harvard and Yale.[119] The continued existence of an Ivy League track to the judiciary ensures that the justices are not from backgrounds or currently in positions that allow them to truly understand what the public and everyday Americans, Justice Harlan's "society," consider reasonable.[120] Additionally, the method of determining a reasonable expectation of privacy is subject to wide variation depending on the methodology used to calculate it.[121] The NSA mass surveillance programs are now public knowledge, so it would be technically unreasonable for the public to maintain a reasonable expectation of privacy in their personal data and electronic communications. Clearly, applying the standard in that way would result in an untenable and absurd result. Nonetheless, that is the very logic that animates the Court's original collapsing of the concepts of secrecy and privacy in *Smith v. Maryland*.[122]

Second, a privacy theory lacks the sort of widespread support across the bench. A successful theory of the Fourth Amendment must appeal to the most conservative common denominator, Justice Scalia. Trespass, as a doctrine, is rooted in the common law and text of the Constitution, which makes it an appealing theory to textualists, originalists, and progressives alike.[123]

V. A Return to the Trespass Theory of the Fourth Amendment Will Restore the Fourth Amendment, Protect the Public, and Increase Faith in Public Institutions

In an era of intrusive domestic surveillance, the Fourth Amendment must be moored in functioning doctrine. The privacy-based theory of the Fourth Amendment as articulated in *Katz* is beyond repair in the digital age. Rather, a more effective way to protect the constitutional rights and privacy of the American public is

118. *See* Nancy Scherer, *Diversifying the Federal Bench: Is Universal Legitimacy for the U.S. Justice System Possible?*, 105 NW. U. L. REV. 587, 587–89 (2011).

119. Biographies of Current Justices of the Supreme Court, http://www.supremecourt.gov/about/biographies.aspx (last visited Apr. 12, 2014).

120. *See* Freiwald, *supra* note 27, at 8.

121. Rubenfeld, *supra* note 36, at 107–08; Kerr, *supra* note 67, at 808.

122. Tomkovicz, *supra* note 112, at 681.

123. *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 786 (1994) (describing origins of trespass in the context of the Fourth Amendment).

to vest Americans with property rights in their personal data and electronic communications. Property rights will form the missing link between the Court's jurisprudence and the expectations of the public. Vesting property rights will transform individuals' legitimate expectations of privacy, which the Court has overlooked, into a tangible form, property rights, which are more easily cognizable by the law and the Court.[124] Property rights in data, including virtual identification information are necessary beyond the context of a fair and efficient marketplace for consumer data, they are necessary to preserve the privacy and Fourth Amendment rights of Americans. Unlike the Court's reasonable expectation of privacy standard, the trespass theory of the Fourth Amendment has withstood the test of time and has been applied to some modern technologies.[125] By vesting property rights in personal data and electronic communications, the courts will have a legal foundation on which to apply a trespass theory of the Fourth Amendment.

Additionally, the legitimacy of the Fourth Amendment and of the judicial system will increase because creating legal ownership of personal data and electronic communications will more accurately reflect the public's sense of ownership and expectations about the use of their data and the internet in general. The legitimacy of our judicial system and the Constitution are inherently important; however, increased legitimacy and respect for these legal institutions will actually benefit the government as well as the public. Although I do not propose, as a matter of policy, that the government continue these programs, their proponents would be wise to support increased Fourth Amendment protections. When members of the public trust the government and view the legal institutions designed to protect them as legitimate, there will be less public outcry and resistance to the very surveillance programs the government seeks to operate to increase national security. By following regulations such as the ECPA and FISA, and operating in a manner that is transparent and legal, the government will be able to maintain its programs, if it so chooses, with less public ire and resistance.

124. *See Smith*, 442 U.S. at 745–46 (holding no reasonable expectation of privacy in information disclosed to third party).

125. *See, e.g.*, *Jones*, 132 S. Ct. at 949; *Kyllo*, 533 U.S. at 40; *Jardines*, 133 S. Ct. at 1413.